Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently amended) A method for communicating passwords comprises:

receiving at a server a challenge from a authentication server via a first secure communications channel, wherein the challenge ~~comprising~~ includes at least a random password from the authentication server that is inactive;

communicating the challenge from the server to a client computer via a second secure communications channel , wherein the client computer receives the random password from the authentication server that is inactive ;

receiving at the server a challenge response from the client computer via the second secure communications channel, wherein the challenge response ~~comprising~~ includes a digital certificate and a digital ~~signature~~ data packet , wherein the digital certificate ~~including~~ includes a public key in an encrypted form, and wherein the digital ~~signature being~~ data packet is determined in the client and ~~response to~~ comprises a combination of at least a portion of the challenge and ~~the~~ a private key corresponding to the public key ; and

communicating the challenge response from the server to the authentication server via the first secure communications channel;

wherein the random password from the authentication server that is inactive is activated when the authentication server verifies the challenge response.

2. (Original) The method of claim 1 wherein the client computer communicates the random password to a password-based security system, the password-based security system coupled to the authentication server.

3. (Original) The method of claim 2 wherein the password-based security system comprises a firewall.

4. (Original) The method of claim 1 wherein the public key and the private key are associated with an authenticated user.

5. (Original) The method of claim 1

wherein the private key is not associated with an authenticated user, and

wherein the authentication server does not authenticate the challenge response.

6. (Currently amended) The method of claim 1 wherein the first secure communications channel is selected from ~~the~~ a group consisting of : secure socket layer and secure HTTP.

7. (Currently amended) A method for a client computer comprises:

receiving challenge data from a authentication server in the client computer via a first secure communications ~~channe~~ channel , wherein the challenge data ~~comprising~~ comprises a challenge and a password from the authentication server that is inactive;

receiving a user PIN;

recovering a private key and a digital certificate in response to the user PIN;

sending the digital certificate to the authentication server via an external server, wherein the digital certificate ~~comprising~~ comprises a public key in an encrypted form;

sending a digital ~~signature~~ data packet to the authentication server via the external server, wherein the digital ~~signature~~ data packet ~~being~~ is determined in the client computer and comprises ~~in response~~ a combination of at least a portion of the challenge and the private key; and thereafter

sending a user login and the password from the authentication server from the client computer to a password-based security system coupled to the authentication server,

wherein when the authentication server verifies the digital ~~signature~~ data packet , the password that is inactive is activated.

8. (Currently amended) The method of claim 7 wherein when the authentication server does not verify the digital ~~signature~~ data packet , the password from the authentication server that is inactive remains inactive.

9. (Currently amended) The method of claim 7 wherein the password-based security system comprises a server selected from ~~the~~ a group consisting of : a firewall and a VPN Gateway.

10. (Original) The method of claim 7 wherein recovering the private key and the digital certificate in response to the user PIN comprises:

recovering a private key associated with the user when the user PIN is correct; and

generating a private key not associated with the user when the user PIN is incorrect.

11. (Currently amended) The method of claim 10 further comprising manually entering the user login and the password from the authentication server to the client computer.

12. (Currently amended) The method of claim 7 wherein the password from the authentication server that is inactive is activated for a pre-determined amount of time.

13. (Currently amended) The method of claim 12 wherein after the pre-determined amount of time, the password from the authentication server that is activated is inactivated.

14. (Currently amended) A method for a verification server comprises:

receiving a request for a one-time password in the verification server from a client computer;

determining a one-time password within the verification server, wherein the one-time password ~~being~~ within the verification server is initially inactive;

communicating data comprising the one-time password that is initially inactive from the verification server to the client computer;

receiving user identification data from a user at the client computer in the verification server ;

verifying in the verification server, the user in response to the user identification data; and

activating the one-time password in the verification serer when the user is ~~authenticated~~ verified .

15. (Currently amended) The method of claim 14 wherein communicating data comprising the one-time password that is initially inactive to the client computer comprises communicating via an external server via a secure communications channel.

16. (Currently amended) The method of claim 14 wherein the one-time password that is initially inactive is selected ~~form the~~ from a group consisting of : random, pre-determined, pseudo-random.

17. (Currently amended) The method of claim 14 wherein the user identification data comprises a digital signature of the one-time password that is initially inactive.

18. (Currently amended) The method of claim 17 wherein the digital signature comprises a private key selected from ~~the~~ a group consisting of : a private key associated with the user, a private key not associated with the user.

19. (Original) The method of claim 18 wherein verifying the user comprises verifying the user when the private key is associated with the user.

20. (Original) The method of claim 14 further comprising:

receiving a verification request from a password-based security system, the verification request comprising a user login and the one-time password;

determining whether the one-time password is activated; and

approving the verification request when the one-time password is determined to be active.